I

(Gesetzgebungsakte)

VERORDNUNGEN

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Kommission,

nach Übermittlung des Entwurfs des Gesetzgebungsaktes an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank ([1]),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Informations- und Kommunikationstechnologien (IKT) unterstützen im digitalen Zeitalter komplexe Systeme, die für alltägliche Aktivitäten eingesetzt werden. Sie sorgen dafür, dass Schlüsselsektoren unserer Volkswirtschaften, einschließlich des Finanzsektors, am Laufen gehalten werden, und verbessern das Funktionieren des Binnenmarkts. Die zunehmende Digitalisierung und Vernetzung verstärken auch das IKT-Risiko, das die Gesellschaft insgesamt — und insbesondere das Finanzsystem — anfälliger für Cyberbedrohungen oder IKT-Störungen macht. Während die allgegenwärtige Nutzung von IKT-Systemen und die hohe Digitalisierung und Konnektivität heute grundlegende Merkmale der Tätigkeiten von Finanzunternehmen der Union sind, muss ihre digitale Resilienz erst noch besser angegangen und in ihre allgemeinen operativen Rahmen integriert werden.

(2) Die Nutzung von IKT hat in den letzten Jahrzehnten einen derart zentralen Stellenwert bei der Erbringung von Finanzdienstleistungen erlangt, dass sie heute entscheidend zur Ausführung typischer alltäglicher Aufgaben aller Finanzunternehmen beiträgt. Auf Digitalisierung beruhen heute beispielsweise Zahlungen, die von bargeld- und papiergestützten Methoden zunehmend auf die Nutzung digitaler Lösungen verlagert wurden, sowie Wertpapierclearing und -abrechnungssysteme, elektronischer und algorithmischer Handel, Darlehens- und Finanzierungsgeschäfte, Peer-to-Peer-Finanzierung, Bonitätseinstufung, Schadensmanagement und Back-Office-

([1]) ABl. C 343 vom 26.8.2021, S. 1.
([2]) ABl. C 155 vom 30.4.2021, S. 38.
([3]) Standpunkt des Europäischen Parlaments 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 28. November 2022.

Transaktionen. Auch der Versicherungssektor hat sich durch den Einsatz von IKT verändert — vom Aufkommen digitaler Versicherungsvermittler, die ihre Dienste online anbieten und mit InsurTech arbeiten, bis hin zu digitalen Versicherungsgeschäften. Das Finanzwesen ist nicht nur sektorweit weitgehend digital geworden, sondern die Digitalisierung hat auch die Verflechtungen und Abhängigkeiten innerhalb des Finanzsektors sowie von Infrastrukturen Dritter und Drittdienstleistern verstärkt.

(3) Der Europäische Ausschuss für Systemrisiken (ESRB) bekräftigte in einem Bericht aus dem Jahr 2020 über systemische Cyberrisiken, wie das bestehende hohe Maß an Verflechtungen zwischen Finanzunternehmen, Finanzmärkten und Finanzmarktinfrastrukturen und insbesondere die gegenseitigen Abhängigkeiten ihrer IKT-Systeme eine Systemanfälligkeit herbeiführen könnten, da lokalisierte Cybervorfälle in einem der rund 22 000 Finanzunternehmen der Union über geografische Grenzen hinweg rasch auf das gesamte Finanzsystem übergreifen könnten. Schwerwiegende IKT-Sicherheitsverletzungen, die im Finanzsektor auftreten können, betreffen nicht nur Finanzunternehmen, die isoliert betrachtet werden. Ebenso können sich hierdurch ermittelte Schwachstellen über die Übertragungskanäle des Finanzsystems verbreiten und die Stabilität des Finanzsystems der Union beeinträchtigen, etwa durch Liquiditätsengpässe und einen allgemeinen Verlust des Vertrauens in die Finanzmärkte.

(4) Politische Entscheidungsträger, Regulierungsbehörden und Normungsgremien auf internationaler Ebene, Unionsebene und nationaler Ebene haben sich in den letzten Jahren mit dem IKT-Risiko befasst, um die digitale Resilienz zu stärken, Standards festzulegen und die Regulierungs- und Aufsichtsarbeit zu koordinieren. Auf internationaler Ebene sind der Basler Ausschuss für Bankenaufsicht, der Ausschuss für Zahlungsverkehr und Marktinfrastrukturen, der Rat für Finanzstabilität, das Institut für Finanzstabilität sowie die G7 und G20 bestrebt, den zuständigen Behörden und Marktteilnehmern in verschiedenen Rechtsordnungen Instrumente an die Hand zu geben, um die Resilienz ihrer Finanzsysteme zu stärken. Diesen Arbeiten lag auch die Notwendigkeit zugrunde, das IKT-Risiko im Kontext eines stark vernetzten globalen Finanzsystems zu berücksichtigen und sich um mehr Kohärenz der relevanten bewährten Verfahren zu bemühen.

(5) Das IKT-Risiko bleibt trotz gezielter politischer und legislativer Initiativen auf Unionsebene und nationaler Ebene eine Herausforderung für die operationale Resilienz, Leistungsfähigkeit und Stabilität des Finanzsystems der Union. Mit den Reformen nach der Finanzkrise von 2008 wurde in erster Linie die finanzielle Resilienz des Finanzsektors der Union gestärkt und darauf abgezielt, die Wettbewerbsfähigkeit und Stabilität der Union aus wirtschaftlicher, aufsichtsrechtlicher und marktpolitischer Sicht zu bewahren. Obwohl IKT-Sicherheit und digitale Resilienz Bestandteil des operationellen Risikos sind, standen sie in der Zeit nach der Finanzkrise weniger im Fokus der Regulierungsagenda und wurden nur in einigen Bereichen der Unionspolitik für Finanzdienstleistungen und Regulierung oder nur in wenigen Mitgliedstaaten weiterentwickelt.

(6) In ihrer Mitteilung mit dem Titel „FinTech-Aktionsplan: für einen wettbewerbsfähigeren und innovativen europäischen Finanzsektor“ vom 8. März 2018 hob die Kommission hervor, wie überaus wichtig es ist, den Finanzsektor der Union widerstandsfähiger zu machen, auch aus operativer Sicht, um seine technologische Sicherheit und sein reibungsloses Funktionieren sowie seine rasche Wiederherstellung nach IKT-Sicherheitsverletzungen und -Vorfällen zu gewährleisten, damit Finanzdienstleistungen in der gesamten Union — auch in Stresssituationen — wirksam und reibungslos erbracht werden können und gleichzeitig das Vertrauen der Verbraucher und der Märkte gewahrt wird.

(7) Im April 2019 veröffentlichten die mit der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([4]) eingerichtete Europäische Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde, EBA), die mit der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates ([5]) eingerichtete Europäische Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung,

([4]) Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

([5]) Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48).

EIOPA) und die mit der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([6]) eingerichtete Europäische Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde, ESMA) (zusammen als „Europäische Aufsichtsbehörden" oder „ESA", im Folgenden „ESA") gemeinsam fachliche Gutachten, in denen ein kohärenter Ansatz für das IKT-Risiko im Finanzbereich gefordert und empfohlen wurde, die digitale operationale Resilienz der Finanzdienstleistungsbranche durch eine sektorspezifische Initiative der Union auf verhältnismäßige Weise zu stärken.

(8) Der Finanzsektor der Union wird durch ein einheitliches Regelwerk (Single Rulebook) reguliert und unterliegt einem europäischen Finanzaufsichtssystem. Dennoch wurden Bestimmungen über die digitale operationale Resilienz und die IKT-Sicherheit noch nicht vollständig oder konsequent harmonisiert, obwohl die digitale operationale Resilienz für die Gewährleistung von Finanzstabilität und Marktintegrität im digitalen Zeitalter von entscheidender Bedeutung und nicht weniger wichtig ist als beispielsweise gemeinsame Aufsichts- oder Marktverhaltensstandards. Daher sollten das einheitliche Regelwerk und das Aufsichtssystem so weiterentwickelt werden, dass sie auch die digitale operationale Resilienz abdecken, indem die Mandate der zuständigen Behörden gestärkt werden, damit sie zur Wahrung der Integrität und der Effizienz des Binnenmarkts und zur Förderung seines ordnungsgemäßen Funktionierens des Managements des IKT-Risikos im Finanzsektor überwachen können.

(9) Rechtliche Unterschiede und ungleiche nationale Regulierungs- oder Aufsichtsansätze in Bezug auf das IKT-Risiko schaffen Hindernisse für das Funktionieren des Binnenmarkts für Finanzdienstleistungen und erschweren grenzüberschreitend tätigen Finanzunternehmen die reibungslose Ausübung der Niederlassungsfreiheit und die Erbringung von Dienstleistungen. Auch der Wettbewerb zwischen denselben Arten von Finanzunternehmen, die in verschiedenen Mitgliedstaaten tätig sind, könnte verzerrt werden. Dies gilt insbesondere in Bereichen, in denen die Harmonisierung auf Unionsebene bislang sehr begrenzt — wie beim Testen der digitalen operationalen Resilienz — oder gar nicht vorhanden ist — wie bei der Überwachung des IKT-Drittparteienrisikos. Unterschiede, die sich aus den auf nationaler Ebene geplanten Entwicklungen ergeben, könnten weitere Hindernisse für das Funktionieren des Binnenmarkts schaffen, die sich nachteilig auf die Marktteilnehmer und die Finanzstabilität auswirken.

(10) Da die einschlägigen Bestimmungen über IKT-Risiken bisher auf Unionsebene nur auf unvollständige Art und Weise angegangen wurden, bestehen Lücken oder Überschneidungen in wichtigen Bereichen — wie der Meldung IKT-bezogener Vorfälle und Tests der digitalen operationalen Resilienz — sowie Unstimmigkeiten aufgrund sich abzeichnender unterschiedlicher nationaler Vorschriften oder einer kostenineffizienten Anwendung sich überschneidender Vorschriften. Dies ist besonders schädlich für intensive IKT-Nutzer wie den Finanzsektor, da technologische Risiken keine Grenzen haben und der Finanzsektor seine Dienste auf breiter grenzüberschreitender Basis inner- und außerhalb der Union erbringt. Einzelne Finanzunternehmen, die grenzüberschreitend tätig sind oder über mehrere Zulassungen verfügen (z. B. kann ein Finanzunternehmen eine Lizenz für eine Bank, eine Wertpapierfirma und ein Zahlungsinstitut besitzen, die jeweils von einer anderen zuständigen Behörde in einem oder mehreren Mitgliedstaaten ausgestellt wurde), stehen bei der alleinigen und kohärenten und kostenwirksamen Bewältigung des IKT-Risikos und der Abmilderung nachteiliger Auswirkungen von IKT-Vorfällen vor operativen Herausforderungen.

(11) Da das einheitliche Regelwerk nicht mit einem umfassenden Rahmen für IKT oder operationelle Risiken einhergeht, ist eine weitere Harmonisierung der wichtigsten Anforderungen an die digitale operationale Resilienz für alle Finanzunternehmen erforderlich. Die Entwicklung der IKT-Kapazitäten und der allgemeinen Resilienz durch Finanzunternehmen auf der Grundlage dieser Kernanforderungen, um operativen Ausfällen standzuhalten, würde dabei helfen, die Stabilität und Integrität der Finanzmärkte der Union zu erhalten, und auf diese Weise dazu beitragen, ein hohes Schutzniveau für Anleger und Verbraucher in der Union sicherzustellen. Da diese Verordnung zum reibungslosen Funktionieren des Binnenmarkts beitragen soll, sollte sie sich auf die Bestimmungen von Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) in der Auslegung der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof") stützen.

(12) Mit dieser Verordnung sollen die Anforderungen mit Blick auf IKT-Risiken im Rahmen der Anforderungen an das operationelle Risiko konsolidiert und verbessert werden, die bisher in verschiedenen Rechtsakten der Union gesondert behandelt wurden. Diese Rechtsakte deckten zwar die wichtigsten Kategorien finanzieller Risiken ab (z. B. Kreditrisiko, Marktrisiko, Gegenparteiausfallrisiko, Liquiditätsrisiko und Marktrisiko), waren aber bei ihrer Annahme nicht umfassend auf alle Komponenten der operationalen Resilienz ausgerichtet. Bei der Weiterentwicklung der Vorschriften über das operationelle Risiko in diesen Rechtsakten der Union wurde häufig ein traditioneller quantitativer Ansatz zur Bewältigung von Risiken (d. h. die Festlegung einer Kapitalvorgabe zur Absicherung gegen

([6]) Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84).

das IKT-Risiko) bevorzugt, anstelle gezielter qualitativer Vorschriften für den Schutz, die Erkennung, Eindämmung, Wiederherstellung und die Sanierungskapazitäten bei IKT-bezogenen Vorfällen oder für die Kapazitäten für Meldungen und Tests digitaler Technologie. Mit diesen Rechtsakten sollten in erster Linie wesentliche Vorschriften über die Beaufsichtigung, die Integrität oder das Verhalten des Marktes abgedeckt und aktualisiert werden. Indem die verschiedenen Vorschriften über IKT-Risiken konsolidiert und verbessert werden, sollten alle Bestimmungen, die sich mit digitalen Risiken im Finanzsektor befassen, erstmals in einheitlicher Weise in einem einzigen Rechtsakt zusammengefasst werden. Somit schließt diese Verordnung Lücken oder behebt Unstimmigkeiten in einigen der vorausgehenden Rechtsakte (auch in Bezug auf die darin verwendete Terminologie) und nimmt durch gezielte Vorschriften über die Kapazitäten für das IKT-Risikomanagement, die Meldung von Vorfällen, Tests der operationalen Resilienz sowie die Überwachung des IKT-Drittparteienrisikos ausdrücklich auf IKT-Risiken Bezug. Somit sollte diese Verordnung auch für das IKT-Risiko sensibilisieren und berücksichtigen, dass die finanzielle Solidität von Finanzunternehmen durch IKT-Vorfälle und eine mangelnde operationale Resilienz beeinträchtigt werden könnten.

(13) Finanzunternehmen sollten bei der Bewältigung von IKT-Risiken denselben Ansatz und dieselben grundsatzbasierten Regeln befolgen, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist. Kohärenz trägt dazu bei, das Vertrauen in das Finanzsystem zu stärken und dessen Stabilität zu erhalten, insbesondere in Zeiten starker Abhängigkeit von IKT-Systemen, -Plattformen und -Infrastrukturen, die erhöhtes digitales Risiko mit sich bringt. Ebenso sollte durch Einhaltung einer grundlegenden Cyberhygiene verhindert werden, dass der Wirtschaft durch die Minimierung der Auswirkungen und Kosten von IKT-Störfällen hohe Kosten entstehen.

(14) Eine Verordnung hilft, die Komplexität der Regulierung zu verringern, fördert die aufsichtliche Konvergenz, erhöht die Rechtssicherheit und trägt ferner dazu bei, die Befolgungskosten, insbesondere für grenzüberschreitend tätige Finanzunternehmen, zu begrenzen und Wettbewerbsverzerrungen zu verringern. Daher ist die Wahl einer Verordnung zur Schaffung eines gemeinsamen Rahmens für die digitale operationale Resilienz von Finanzunternehmen am besten geeignet, eine einheitliche und kohärente Anwendung aller Komponenten des IKT-Risikomanagements im Finanzsektor der Union zu gewährleisten.

(15) Die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([7]) stellte den ersten horizontalen Rahmen für die Cybersicherheit auf Unionsebene dar, der auch für drei Arten von Finanzunternehmen, namentlich für Kreditinstitute, Handelsplätze und zentrale Gegenparteien gilt. Da in der Richtlinie (EU) 2016/1148 jedoch ein Mechanismus zur Identifizierung der Betreiber wesentlicher Dienste auf nationaler Ebene vorgesehen ist, wurden nur bestimmte Kreditinstitute, Handelsplätze und zentrale Gegenparteien, die von den Mitgliedstaaten ermittelt wurden, in der Praxis in den Anwendungsbereich der Richtlinie aufgenommen und daher verpflichtet, die darin festgelegten Anforderungen an die IKT-Sicherheit und die Meldung von Vorfällen zu erfüllen. Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([8]) legt ein einheitliches Kriterium dafür fest, welche Unternehmen in ihren Anwendungsbereich fallen (Schwellenwert für die Größe), wobei auch die drei Arten von Finanzunternehmen in ihrem Anwendungsbereich verbleiben.

(16) Da mit dieser Verordnung jedoch das Ausmaß der Harmonisierung in Bezug auf die verschiedenen Komponenten der digitalen Resilienz erhöht wird, indem Anforderungen an das IKT-Risikomanagement und die Meldung von IKT-Vorfällen eingeführt werden, die strenger sind als diejenigen im aktuellen Finanzdienstleistungsrecht der Union, stellt dies auch im Vergleich zu den Anforderungen der Richtlinie (EU) 2022/2555 eine stärkere Harmonisierung dar. Folglich verkörpert diese Verordnung eine *Lex specialis* zur Richtlinie (EU) 2022/2555. Es ist zugleich von entscheidender Bedeutung, dass eine enge Beziehung zwischen dem Finanzsektor und dem derzeit in der Richtlinie (EU) 2022/2555 festgelegten horizontalen Rahmen der Union für Cybersicherheit aufrechterhalten wird, um die Kohärenz mit den von den Mitgliedstaaten angenommenen Strategien für Cybersicherheit zu gewährleisten und es Finanzaufsichtsbehörden zu ermöglichen, auf Cybervorfälle aufmerksam gemacht zu werden, die andere unter die genannte Richtlinie fallende Sektoren betreffen.

([7]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

([8]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (siehe Seite 80 dieses Amtsblatts).

(17) Im Einklang mit Artikel 4 Absatz 2 des Vertrags über die Europäische Union und unbeschadet der gerichtlichen Überprüfung durch den Gerichtshof sollte diese Verordnung die Zuständigkeit der Mitgliedstaaten für die grundlegenden Funktionen des Staates in Bezug auf die öffentliche Sicherheit, die Verteidigung und den Schutz der nationalen Sicherheit — z. B. in Bezug auf die Bereitstellung von Informationen, die dem Schutz der nationalen Sicherheit zuwiderlaufen würden — unberührt lassen.

(18) Um sektorübergreifendes Lernen zu ermöglichen und Erfahrungen anderer Sektoren beim Umgang mit Cyberbedrohungen wirksam zu nutzen, sollten Finanzunternehmen im Sinne der Richtlinie (EU) 2022/2555 Teil des „Ökosystems" jener Richtlinie bleiben (z. B. Kooperationsgruppe und Computer-Notfallteam (computer security incident response team, CSIRT)). Die ESA und zuständige nationale Behörden sollten in der Lage sein, sich an den strategischen politischen Diskussionen und der technischen Arbeit der Kooperationsgruppe im Sinne der genannten Richtlinie zu beteiligen, Informationen austauschen und mit den entsprechend der genannten Richtlinie benannten oder eingerichteten zentralen Anlaufstellen weiter zusammenarbeiten. Die nach der vorliegenden Verordnung zuständigen Behörden sollten auch die CSIRT konsultieren und mit ihnen zusammenarbeiten. Darüber hinaus sollten die zuständigen Behörden die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden um fachliche Beratung ersuchen und Kooperationsvereinbarungen schließen können, mit denen wirksame und schnelle Koordinierungsmechanismen sichergestellt werden sollen.

(19) Angesichts der engen Verflechtungen zwischen der digitalen Resilienz und der physischen Resilienz von Finanzunternehmen ist in der vorliegenden Verordnung und in der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates ([9]) ein kohärenter Ansatz in Bezug auf die Resilienz kritischer Einrichtungen erforderlich. Da das IKT-Risikomanagement und die Meldepflichten nach der vorliegenden Verordnung der physischen Resilienz von Finanzunternehmen umfassend Rechnung tragen, sollten die in den Kapiteln III und IV der Richtlinie (EU) 2022/2557 festgelegten Verpflichtungen nicht für Finanzunternehmen gelten, die in den Anwendungsbereich der genannten Richtlinie fallen.

(20) Anbieter von Cloud-Computing-Diensten sind eine Kategorie digitaler Infrastruktur, die unter die Richtlinie (EU) 2022/2555 fällt. Der mit dieser Verordnung geschaffene Überwachungsrahmen der Union (im Folgenden „Überwachungsrahmen") gilt für alle kritischen IKT-Drittdienstleister, einschließlich Anbietern von Cloud-Computing-Diensten, die Finanzunternehmen IKT-Dienstleistungen bereitstellen, und sollte als Ergänzung zu der Beaufsichtigung gemäß der Richtlinie (EU) 2022/2555 betrachtet werden. Darüber hinaus sollte der mit dieser Verordnung geschaffene Überwachungsrahmen für Anbieter von Cloud-Computing-Diensten gelten, wenn es keinen horizontalen Rahmen der Union gibt, mit dem eine Behörde für die digitale Überwachung eingerichtet wird.

(21) Um die vollständige Kontrolle über das IKT-Risiko zu behalten, müssen Finanzunternehmen über umfassende Kapazitäten verfügen, die ein leistungsfähiges und wirksames IKT-Risikomanagement sowie spezifische Mechanismen und Strategien für die Handhabung aller IKT-bezogener Vorfälle und für die Meldung schwerwiegender IKT-bezogener Vorfälle ermöglichen. Ebenso sollten Finanzunternehmen über Leit- und Richtlinien für die Erprobung von IKT-Systemen, -Kontrollen und -Prozessen sowie für das Management des IKT-Drittparteienrisikos verfügen. Die Mindestanforderungen an die digitale operationale Resilienz für Finanzunternehmen sollten angehoben werden, wobei auch eine verhältnismäßige Anwendung der Anforderungen für bestimmte Finanzunternehmen möglich sein sollte, insbesondere bei Kleinstunternehmen sowie Finanzunternehmen, die einem vereinfachten IKT-Risikomanagementrahmen unterliegen. Um eine effiziente Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung zu ermöglichen, die verhältnismäßig ist und der Notwendigkeit Rechnung trägt, den Verwaltungsaufwand für die zuständigen Behörden zu verringern, sollten die einschlägigen nationalen Aufsichtsmechanismen für derartige Finanzunternehmen deren Größe und Gesamtrisikoprofil sowie die Art, den Umfang und die Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte berücksichtigen, auch wenn die in Artikel 5 der Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates ([10]) festgelegten einschlägigen Schwellenwerte überschritten werden. Insbesondere sollten sich die Aufsichtstätigkeiten vorrangig auf die Notwendigkeit konzentrieren, ernsthaften Risiken im Zusammenhang mit dem IKT-Risikomanagement eines bestimmten Unternehmens entgegenzuwirken.

([9]) Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (siehe Seite 164 dieses Amtsblatts).

([10]) Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates vom 14. Dezember 2016 über die Tätigkeiten und die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung (EbAV) (ABl. L 354 vom 23.12.2016, S. 37).

Die zuständigen Behörden sollten auch einen wachsamen, aber verhältnismäßigen Ansatz in Bezug auf die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung verfolgen, die gemäß Artikel 31 der Richtlinie (EU) 2016/2341 einen wesentlichen Teil ihres Kerngeschäfts, wie Vermögensverwaltung, versicherungsmathematische Berechnungen, Rechnungslegung und Datenverwaltung, an Dienstleister auslagern.

(22) Die Schwellenwerte und Taxonomien für die Meldung IKT-bezogener Vorfälle unterscheiden sich auf nationaler Ebene erheblich. Wenngleich sich durch einschlägige Arbeiten der durch die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([11]) eingerichtete Agentur der Europäischen Union für Cybersicherheit (ENISA) und der Kooperationsgruppe im Sinne der Richtlinie (EU) 2022/2555 eine gemeinsame Grundlage schaffen lässt, bestehen für die übrigen Finanzunternehmen noch immer unterschiedliche Ansätze in Bezug auf die Festlegung der Schwellenwerte und die Verwendung von Taxonomien bzw. können sich für diese ergeben. Aufgrund dieser Unterschiede besteht eine Vielzahl von Anforderungen, die Finanzunternehmen einhalten müssen, insbesondere wenn sie in mehreren Mitgliedstaaten tätig sind und Teil einer Finanzgruppe sind. Darüber hinaus können derartige Unterschiede die Einrichtung weiterer einheitlicher oder zentralisierter Mechanismen der Union behindern, die das Meldeverfahren beschleunigen und einen raschen und reibungslosen Informationsaustausch zwischen den zuständigen Behörden unterstützen, was für die Bewältigung des IKT-Risikos bei Großangriffen mit potenziell systemischen Folgen von entscheidender Bedeutung ist.

(23) Um für bestimmte Finanzunternehmen den Verwaltungsaufwand zu verringern und potenziell doppelte Meldepflichten zu vermeiden, sollte die Verpflichtung zur Meldung von Vorfällen gemäß der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates ([12]) nicht mehr für Zahlungsdienstleister gelten, die in den Geltungsbereich dieser Verordnung fallen. Folglich sollten Kreditinstitute, E-Geld-Institute, Zahlungsinstitute und Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der genannten Richtlinie alle zahlungsbezogenen Betriebs- oder Sicherheitsvorfälle, die vormals gemäß der genannten Richtlinie gemeldet wurden, ab dem Geltungsbeginn dieser Verordnung gemäß dieser melden, und zwar unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht.

(24) Um den zuständigen Behörden die Erfüllung von Aufsichtsaufgaben zu ermöglichen, indem sie einen vollständigen Überblick über Art, Häufigkeit, Ausmaß und Auswirkungen IKT-bezogener Vorfälle erhalten, und um den Informationsaustausch zwischen einschlägigen Behörden, einschließlich Strafverfolgungs- und Abwicklungsbehörden, zu verbessern, sollte diese Verordnung eine solide Regelung für die Meldung IKT-bezogener Vorfälle festlegen, wobei die einschlägigen Anforderungen derzeitige Lücken im Finanzdienstleistungsrecht schließen, und Überschneidungen und Doppelarbeit mit Blick auf eine Senkung der Kosten beseitigen. Es ist von entscheidender Bedeutung, die Regelung für die Meldung IKT-bezogener Vorfälle zu harmonisieren, indem alle Finanzunternehmen verpflichtet werden, ihren zuständigen Behörden in dem in dieser Verordnung vorgesehenen einheitlichen, gestrafften Rahmen Bericht zu erstatten. Darüber hinaus sollten die ESA ermächtigt werden, relevante Aspekte für den Rahmen für die Meldung IKT-bezogener Vorfälle — wie Taxonomie, Zeitrahmen, Datensätze, Vorlagen und anwendbare Schwellenwerte — näher zu spezifizieren. Um vollständige Übereinstimmung mit der Richtlinie (EU) 2022/2555 zu gewährleisten, sollten Finanzunternehmen der jeweils zuständigen Behörde auf freiwilliger Basis erhebliche Cyberbedrohungen melden können, wenn sie der Auffassung sind, dass die Cyberbedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist.

(25) In einigen Teilsektoren des Finanzsektors wurden Anforderungen für Tests der digitalen operationalen Resilienz entwickelt, deren Rahmen nicht immer vollständig aneinander angeglichen waren. Dies führt zu potenziell doppelten Kosten für grenzüberschreitend tätige Finanzunternehmen und verkompliziert die gegenseitige Anerkennung der Ergebnisse von Tests der digitalen operationalen Resilienz, was wiederum zu einer Fragmentierung des Binnenmarkts führen könnte.

([11]) Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

([12]) Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

(26) Darüber hinaus bleiben Schwachstellen, wenn keine IKT-Tests vorgeschrieben sind, unentdeckt, wodurch ein Finanzunternehmen IKT-Risiken ausgesetzt wird und letztlich ein höheres Risiko für die Stabilität und Integrität des Finanzsektors entsteht. Ohne ein Tätigwerden der Union wären Tests der digitalen operationalen Resilienz weiterhin uneinheitlich, und es gäbe kein System für die gegenseitige Anerkennung der IKT-Testergebnisse in verschiedenen Rechtsordnungen. Da es unwahrscheinlich ist, dass Testregelungen in anderen Teilsektoren des Finanzsektors in bedeutendem Umfang eingeführt würden, gingen darüber hinaus die potenziellen Vorteile eines Rahmens für Tests im Hinblick auf die Aufdeckung von Schwachstellen und Risiken sowie von Tests von Verteidigungsfähigkeiten und die Fortführung der Geschäftstätigkeit verloren, die zur Stärkung des Vertrauens von Kunden, Lieferanten und Geschäftspartnern beitragen. Um diese Überschneidungen, Divergenzen und Lücken zu beseitigen, müssen Vorschriften für ein koordiniertes Testsystem festgelegt werden, damit die gegenseitige Anerkennung erweiterter Tests für diejenigen Finanzunternehmen erleichtert wird, die die Kriterien in dieser Verordnung erfüllen.

(27) Die Abhängigkeit der Finanzunternehmen von IKT-Dienstleistungen ist zum Teil darauf zurückzuführen, dass sie sich an eine sich entwickelnde wettbewerbsorientierte digitale Weltwirtschaft anpassen, ihre geschäftliche Effizienz steigern und die Verbrauchernachfrage befriedigen müssen. Die Art und das Ausmaß dieser Nutzung von IKT-Dienstleistungen haben sich in den letzten Jahren ständig weiterentwickelt, was zu Kostensenkungen bei der Finanzintermediation geführt hat, die Expansion von Unternehmen und die Skalierbarkeit bei der Ausübung von Finanztätigkeiten ermöglicht und gleichzeitig ein breites Spektrum an IKT-Tools für die Verwaltung komplexer interner Prozesse zur Verfügung gestellt hat.

(28) Die umfangreiche Nutzung von IKT-Dienstleistungen zeigt sich an komplexen vertraglichen Vereinbarungen, wobei Finanzunternehmen häufig Schwierigkeiten haben, Vertragsbedingungen auszuhandeln, die auf die Aufsichtsstandards oder sonstige aufsichtsrechtliche Anforderungen, denen sie unterliegen, zugeschnitten sind; Gleiches gilt für die Durchsetzung bestimmter Rechte, wie Zugangs- oder Auditrechte, selbst wenn diese in ihren vertraglichen Vereinbarungen verankert sind. Darüber hinaus fehlen in vielen dieser vertraglichen Vereinbarungen ausreichende Garantien, die die vollständige Überwachung von Verfahren für die Unterauftragsvergabe ermöglichen, wodurch das Finanzunternehmen die damit verbundenen Risiken nicht bewerten kann. Da IKT-Drittdienstleister häufig standardisierte Dienstleistungen für verschiedene Arten von Kunden anbieten, wird den individuellen oder spezifischen Bedürfnissen der Akteure der Finanzbranche in derartigen vertraglichen Vereinbarungen nicht immer angemessen Rechnung getragen.

(29) Obwohl die Rechtsvorschriften für Finanzdienstleistungen bestimmte allgemeine Vorschriften über die Auslagerung von Tätigkeiten enthalten, ist die Überwachung der vertraglichen Dimension nicht vollständig in den Rechtsvorschriften der Union verankert. Weil eindeutige und angepasste Unionsstandards, die auf die vertraglichen Vereinbarungen mit IKT-Drittdienstleistern anwendbar sind, fehlen, werden externe Quellen für IKT-Risiken nicht umfassend behandelt. Daher müssen bestimmte Schlüsselprinzipien festgelegt werden, die Finanzunternehmen als Richtschnur für das Management des IKT-Drittparteienrisikos dienen und von besonderer Bedeutung sind, wenn Finanzunternehmen zur Unterstützung ihrer kritischen oder wichtigen Funktionen auf IKT-Drittdienstleister zurückgreifen. Diese Prinzipien sollten mit einer Reihe grundlegender vertraglicher Rechte einhergehen, die sich auf mehrere Aspekte bei der Erfüllung und Beendigung von vertraglichen Vereinbarungen beziehen, damit bestimmte Mindestgarantien geboten werden, um die Fähigkeit von Finanzunternehmen, alle von Drittdienstleistern ausgehenden IKT-Risiken wirksam zu überwachen, zu stärken. Diese Prinzipien ergänzen die für die Auslagerung geltenden sektorspezifischen Rechtsvorschriften.

(30) Ein gewisser Mangel an Homogenität und Konvergenz in Bezug auf die Überwachung des IKT-Drittparteienrisikos und die Abhängigkeit von IKT-Drittdienstleistern ist derzeit festzustellen. Obwohl Anstrengungen unternommen wurden, um den Bereich der Auslagerung anzugehen, wie beispielsweise die Leitlinien der EBA zu Auslagerung von 2019 und Leitlinien der ESMA zur Auslagerung an Cloud-Anbieter von 2021, wird die allgemeinere Frage der Eindämmung systemischer Risiken, die entstehen könnten, wenn der Finanzsektor einer begrenzten Anzahl kritischer IKT-Drittdienstleister ausgesetzt ist, im Unionsrecht nicht ausreichend behandelt. Der Mangel an Vorschriften auf Unionsebene wird noch dadurch verschärft, dass es keine nationalen Vorschriften für die Mandate und Instrumente gibt, die es Finanzaufsichtsbehörden ermöglichen, Abhängigkeiten von IKT-Drittdienstleistern ordnungsgemäß zu erfassen und Risiken, die sich aus der Konzentration der Abhängigkeiten von IKT-Drittdienstleistern ergeben, angemessen zu überwachen.

(31) Unter Berücksichtigung der potenziellen Systemrisiken, die mit der verstärkten Auslagerung und der Konzentration der Abhängigkeiten von IKT-Drittdienstleistern verbunden sind, und in Anbetracht nationaler Regelungen, die den Finanzaufsichtsbehörden unzureichend Werkzeuge bereitstellen, die geeignet sind, die Folgen der bei kritischen IKT-Drittdienstleistern auftretenden IKT-Risiken zu quantifizieren, zu qualifizieren und zu beheben, muss ein geeigneter Überwachungsrahmen geschaffen werden, der eine kontinuierliche Überwachung der Tätigkeiten von IKT-Drittdienstleistern, bei denen es sich um für Finanzunternehmen kritische IKT-Drittdienstleister handelt, ermöglicht und zugleich bei Kunden, bei denen es sich nicht um Finanzunternehmen handelt, Vertraulichkeit und Sicherheit gewährleistet. Auch wenn mit der gruppeninternen Bereitstellung von IKT-Dienstleistungen spezifische Risiken und Vorteile einhergehen, sollte sie nicht automatisch als weniger riskant angesehen werden als die Bereitstellung von IKT-Dienstleistungen durch Dienstleister außerhalb einer Finanzgruppe und sollte daher demselben Rechtsrahmen unterliegen. Wenn IKT-Dienstleistungen innerhalb einer Finanzgruppe bereitgestellt werden, könnten Finanzunternehmen möglicherweise jedoch ein höheres Maß an Kontrolle über gruppeninterne Dienstleister haben, was bei der Gesamtrisikobewertung berücksichtigt werden sollte.

(32) Da IKT- Risiken immer komplexer und technisch ausgereifter werden, hängen gute Maßnahmen für die Erkennung und Prävention von IKT-Risiken in hohem Maße von einem regelmäßigen Informationsaustausch zwischen Finanzunternehmen über Bedrohungen und Schwachstellen ab. Ein Informationsaustausch trägt dazu bei, das Bewusstsein für Cyberbedrohungen zu schärfen. Dies wiederum verstärkt die Fähigkeit der Finanzunternehmen, zu verhindern, dass Cyberbedrohungen in reale IKT-bezogene Vorfälle münden, und versetzt Finanzunternehmen in die Lage, die Auswirkungen IKT-bezogener Vorfälle wirksamer einzudämmen und sich schneller zu erholen. In Ermangelung von Leitlinien auf Unionsebene scheinen mehrere Faktoren einen solchen Wissensaustausch verhindert zu haben, darunter insbesondere die Unsicherheit hinsichtlich der Vereinbarkeit mit den Datenschutz-, Kartell- und Haftungsvorschriften.

(33) Darüber hinaus führen Zweifel bezüglich der Art von Informationen, die mit anderen Marktteilnehmern oder mit Nicht-Aufsichtsbehörden (z. B. ENISA für analytische Eingaben oder Europol für Strafverfolgungszwecke) ausgetauscht werden können, dazu, dass nützliche Informationen vorenthalten werden. Deswegen sind Umfang und Qualität des Informationsaustauschs derzeit nach wie vor begrenzt und fragmentiert, wobei der einschlägige Austausch hauptsächlich auf lokaler Ebene (über nationale Initiativen) erfolgt und keine einheitlichen unionsweiten Regelungen für den Informationsaustausch bestehen, die auf die Bedürfnisse eines integrierten Finanzsystems zugeschnitten sind. Aus diesem Grund ist es wichtig, diese Kommunikationskanäle zu stärken.

(34) Finanzunternehmen sollten ermutigt werden, Informationen und Erkenntnisse zu Cyberbedrohungen untereinander auszutauschen und ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen, abzuwehren und auf sie zu reagieren, indem sie an Vereinbarungen über den Austausch von Informationen teilnehmen. Daher muss auf Unionsebene die Einrichtung von Regelungen für freiwillige Vereinbarungen über den Informationsaustausch ermöglicht werden, die — bei der Umsetzung in vertrauenswürdigen Umgebungen — der Finanzwelt dabei helfen würden, Cyberbedrohungen vorzubeugen und gemeinsam auf diese zu reagieren, indem die Ausbreitung von IKT-Risiken rasch eingedämmt und potenzielle Ansteckungseffekte über alle Finanzkanäle hinweg verhindert werden. Diese Regelungen sollten mit dem anwendbaren Wettbewerbsrecht der Union, das in der Mitteilung der Kommission vom 14. Januar 2011 mit dem Titel „Leitlinien zur Anwendbarkeit des Artikels 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit“ sowie den Datenschutzvorschriften der Union und insbesondere der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([13]) im Einklang stehen. Sie sollten auf der Grundlage einer oder mehrerer der in Artikel 6 jener Verordnung festgelegten Rechtsgrundlagen tätig werden, beispielsweise im Zusammenhang mit der Verarbeitung personenbezogener Daten, die zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten gemäß Artikel 6 Absatz 1 Buchstabe f jener Verordnung erforderlich ist, sowie im Zusammenhang mit der Verarbeitung personenbezogener Daten, die für die Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, gemäß Artikel 6 Absatz 1 Buchstabe c bzw. e jener Verordnung erforderlich ist.

([13]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), (ABl. L 119 vom 4.5.2016, S. 1).

(35) Um ein hohes Niveau an digitaler operationaler Resilienz im gesamten Finanzsektor aufrechtzuerhalten und zugleich mit den technologischen Entwicklungen Schritt zu halten, sollte in der vorliegenden Verordnung auf Risiken eingegangen werden, die sich aus allen Arten von IKT-Dienstleistungen ergeben. Zu diesem Zweck sollte die Definition von IKT-Dienstleistungen im Zusammenhang mit der vorliegenden Verordnung weit ausgelegt werden und digitale Dienste und Datendienste umfassen, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern fortlaufend bereitgestellt werden. Diese Definition sollte beispielsweise sogenannte „Over-the-top"-Dienste umfassen, die unter die Kategorie der elektronischen Kommunikationsdienste fallen. Sie sollte nur die begrenzte Kategorie traditioneller analoger Telefondienste ausschließen, die als Dienste des öffentlichen Fernsprechnetzes (PSTN — Public Switched Telephone Network), Festnetz-Dienste, herkömmliche Fernsprechdienste (POTS — Plain Old Telephone Service) oder Festnetztelefondienste gelten.

(36) Ungeachtet des in dieser Verordnung vorgesehenen breiten Geltungsbereichs sollten bei der Anwendung der Vorschriften für die digitale operationale Resilienz die wesentlichen Unterschiede zwischen Finanzunternehmen in Bezug auf deren Größe und Gesamtrisikoprofil berücksichtigt werden. Als Grundprinzip sollten Finanzunternehmen bei der Verteilung von Ressourcen und Kapazitäten für die Umsetzung des Rahmens für das IKT-Risikomanagement ihren IKT-Bedarf sorgfältig auf ihre Größe und ihr Gesamtrisikoprofil sowie die Art, den Umfang und die Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte abstimmen, während die zuständigen Behörden den Ansatz einer solchen Verteilung weiterhin bewerten und überprüfen sollten.

(37) Die in Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 genannten Kontoinformationsdienstleister werden unter Berücksichtigung der Besonderheiten ihrer Tätigkeiten und der mit ihnen verbundenen Risiken ausdrücklich in den Geltungsbereich der vorliegenden Verordnung einbezogen. Darüber hinaus fallen gemäß Artikel 9 Absatz 1 der Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates ([14]) und Artikel 32 Absatz 1 der Richtlinie (EU) 2015/2366 ausgenommene E-Geld-Institute und Zahlungsinstitute auch dann in den Geltungsbereich dieser Verordnung, wenn ihnen keine Zulassung gemäß der Richtlinie 2009/110/EG für die Ausgabe von E-Geld erteilt wurde oder wenn ihnen keine Zulassung für die Erbringung und Ausführung von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 erteilt wurde. Postscheckämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates ([15]) sind jedoch vom Geltungsbereich der vorliegenden Verordnung ausgenommen. Die zuständige Behörde für die nach der Richtlinie (EU) 2015/2366 ausgenommenen Zahlungsinstitute, die nach der Richtlinie 2009/110/EG ausgenommenen E-Geld-Institute und die Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 sollte die gemäß Artikel 22 der Richtlinie (EU) 2015/2366 benannte zuständige Behörde sein.

(38) Da größere Finanzunternehmen unter Umständen über umfangreichere Ressourcen verfügen und rasch Mittel für die Einrichtung von Governance-Strukturen und die Einführung verschiedener Unternehmensstrategien bereitstellen könnten, sollten nur Finanzunternehmen, die keine Kleinstunternehmen im Sinne dieser Verordnung sind, verpflichtet werden, komplexere Governance-Regelungen einzuführen. Diese Unternehmen sind besser gerüstet, um insbesondere spezielle Managementfunktionen für die Überwachung von Vereinbarungen mit IKT-Drittdienstleistern oder für den Umgang mit dem Krisenmanagement einzurichten, ihr IKT-Risikomanagement nach dem Modell der drei Verteidigungslinien zu strukturieren oder ein internes Modell für Risikomanagement und Kontrolle einzuführen und ihren IKT-Risikomanagementrahmen internen Revisionen zu unterziehen.

(39) Einige Finanzunternehmen kommen in den Genuss von Ausnahmen oder unterliegen gemäß dem einschlägigen sektorspezifischen Unionsrecht einem sehr lockeren Regelungsrahmen. Zu diesen Finanzunternehmen zählen Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates ([16]), Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates ([17]) und Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt nicht mehr als 15 Versorgungs-

([14]) Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (ABl. L 267 vom 10.10.2009, S. 7).

([15]) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

([16]) Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 über die Verwalter alternativer Investmentfonds und zur Änderung der Richtlinien 2003/41/EG und 2009/65/EG und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 1095/2010 (ABl. L 174 vom 1.7.2011, S. 1).

([17]) Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

anwärtern betreiben. Angesichts dieser Ausnahmen wäre es nicht verhältnismäßig, diese Finanzunternehmen in den Geltungsbereich der vorliegenden Verordnung aufzunehmen. Darüber hinaus wird in der vorliegenden Verordnung den strukturellen Besonderheiten des Versicherungsvermittlermarkts Rechnung getragen, sodass Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, die als Kleinstunternehmen oder als kleine oder mittlere Unternehmen gelten, nicht unter diese Verordnung fallen sollten.

(40) Da die in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU genannten Einrichtungen vom Anwendungsbereich jener Richtlinie ausgenommen sind, sollten die Mitgliedstaaten beschließen können, diejenigen dieser Einrichtungen, die sich in ihrem jeweiligen Hoheitsgebiet befinden, von der Anwendung dieser Verordnung auszunehmen.

(41) Um diese Verordnung an den Anwendungsbereich der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([18]) anzugleichen, ist es auch angezeigt, diejenigen in Artikel 2 und 3 jener Richtlinie genannten natürlichen und juristischen Personen, die Wertpapierdienstleistungen erbringen dürfen, ohne eine Zulassung gemäß der genannten Richtlinie erhalten zu müssen, vom Geltungsbereich der vorliegenden Verordnung auszunehmen. Nach Artikel 2 der Richtlinie 2014/65/EU sind jedoch auch Unternehmen, die für die Zwecke der vorliegenden Verordnung als Finanzunternehmen gelten, wie Zentralverwahrer, Organismen für gemeinsame Anlagen oder Versicherungs- und Rückversicherungsunternehmen, vom Anwendungsbereich der genannten Richtlinie ausgenommen. Die Ausnahme der in den Artikeln 2 und 3 jener Richtlinie genannten Personen und Unternehmen vom Geltungsbereich der vorliegenden Verordnung sollte nicht für diese Zentralverwahrer, Organismen für gemeinsame Anlagen oder Versicherungs- und Rückversicherungsunternehmen gelten.

(42) Nach dem sektorspezifischen Unionsrecht unterliegen einige Finanzunternehmen aufgrund ihrer Größe oder den von ihnen erbrachten Dienstleistungen weniger strengen Anforderungen oder Ausnahmen. Diese Kategorie von Finanzunternehmen umfasst auch kleine und nicht verflochtene Wertpapierfirmen, kleine Einrichtungen der betrieblichen Altersversorgung, die unter den in Artikel 5 der Richtlinie (EU) 2016/2341 festgelegten Bedingungen durch die betroffenen Mitgliedstaaten vom Anwendungsbereich jener Richtlinie ausgenommen werden können und Altersversorgungssysteme betreiben, die zusammen nicht mehr als 100 Mitglieder haben, sowie gemäß der Richtlinie 2013/36/EU ausgenommene Institute. Im Einklang mit dem Grundsatz der Verhältnismäßigkeit und zur Wahrung des Geistes des sektorspezifischen Unionsrechts ist es daher auch angezeigt, diese Finanzunternehmen durch die vorliegende Verordnung einem vereinfachten IKT-Risikomanagementrahmen zu unterwerfen. Die Verhältnismäßigkeit des IKT-Risikomanagementrahmens für diese Finanzunternehmen sollte durch die von den ESA zu entwickelnden technischen Regulierungsstandards nicht verändert werden. Darüber hinaus ist es im Einklang mit dem Grundsatz der Verhältnismäßigkeit angezeigt, durch die vorliegende Verordnung auch Zahlungsinstitute im Sinne des Artikels 32 Absatz 1 der Richtlinie (EU) 2015/2366 und E-Geld-Institute im Sinne des Artikels 9 der Richtlinie 2009/110/EG, die gemäß dem nationalen Recht, das diese Rechtsakte der Union umsetzt, ausgenommen sind, einem vereinfachten IKT-Risikomanagementrahmen zu unterwerfen, während Zahlungsinstitute und E-Geld-Institute, die gemäß der jeweiligen Umsetzung des sektorspezifischen Unionsrechts nicht ausgenommen wurden, den in der vorliegenden Verordnung festgelegten allgemeinen Rahmen einhalten sollten.

(43) Ebenso sollten Finanzunternehmen, die als Kleinstunternehmen gelten oder dem vereinfachten IKT-Risikomanagementrahmen nach dieser Verordnung unterliegen, nicht verpflichtet sein, eine Funktion zur Überwachung ihrer mit IKT-Drittdienstleistern geschlossenen Vereinbarungen über die Nutzung von IKT-Dienstleistungen einzurichten oder ein Mitglied der Geschäftsleitung zu benennen, das für die Überwachung der damit verbundenen Risikoexposition und die einschlägige Dokumentation zuständig ist, die Verantwortung für das Management und die Überwachung von IKT-Risiken einer Kontrollfunktion zuzuweisen und zur Vermeidung von Interessenkonflikten ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicherzustellen, den IKT-Risikomanagementrahmen mindestens einmal jährlich zu dokumentieren und zu überprüfen, den IKT-Risikomanagementrahmen regelmäßig einer internen Revision zu unterziehen, nach größeren Veränderungen ihrer Netzwerk- und Informationssysteminfrastrukturen und -prozesse eingehende Bewertungen durchzuführen, regelmäßig Risikoanalysen von IKT-Altsystemen vorzunehmen, die Umsetzung der IKT-Reaktions- und Wiederherstellungspläne einer unabhängigen internen Revision zu unterziehen, eine Krisenmanagementfunktion festzulegen, die Tests der Geschäftsfortführungspläne und der Reaktions- und Wiederherstellungspläne zur Erfassung von Szenarien für die Umstellung von primärer IKT-Infrastruktur auf redundante Systeme auszuweiten, den zuständigen Behörden auf deren Anfrage eine

([18]) Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

Schätzung der von schwerwiegenden IKT-bezogenen Vorfällen verursachten aggregierten jährlichen Kosten und Verluste vorzulegen, redundante IKT-Kapazitäten zu unterhalten, den zuständigen nationalen Behörden die nach nachträglichen Prüfungen IKT-bezogener Vorfälle vorgenommenen Änderungen zu melden, die einschlägigen technologischen Entwicklungen fortlaufend zu überwachen, als integralen Bestandteil des in dieser Verordnung vorgesehenen IKT-Risikomanagementrahmens ein umfassendes Programm für Tests der digitalen operationalen Resilienz einzurichten oder eine Strategie für das IKT-Drittparteienrisiko zu verabschieden und regelmäßig zu überprüfen. Darüber hinaus sollten Kleinstunternehmen nur verpflichtet sein, auf der Grundlage ihres Risikoprofils zu bewerten, ob diese redundanten IKT-Kapazitäten unterhalten werden müssen. Kleinstunternehmen sollten in den Genuss einer flexibleren Regelung für Programme für Tests der digitalen operationalen Resilienz kommen. Bei der Erwägung der Art und Häufigkeit der durchzuführenden Tests sollten sie ein angemessenes Gleichgewicht zwischen dem Ziel der Aufrechterhaltung einer hohen digitalen operationalen Resilienz, den verfügbaren Ressourcen und ihrem Gesamtrisikoprofil finden. Kleinstunternehmen und Finanzunternehmen, die dem vereinfachten IKT-Risikomanagementrahmen nach dieser Verordnung unterliegen, sollten von der Verpflichtung ausgenommen werden, erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis bedrohungsorientierter Penetrationstests (TLPT — Threat Led Penetration Testing) durchzuführen, da nur Finanzunternehmen, die die Kriterien in dieser Verordnung erfüllen, verpflichtet sein sollten, diese Tests durchzuführen. Angesichts ihrer begrenzten Kapazitäten sollten Kleinstunternehmen mit dem IKT-Drittdienstleister vereinbaren können, die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens an einen vom IKT-Drittdienstleister zu beauftragenden unabhängigen Dritten zu delegieren, sofern das Finanzunternehmen jederzeit alle relevanten Informationen und Zusicherungen über die Leistung des IKT-Drittdienstleisters von dem jeweiligen unabhängigen Dritten anfordern kann.

(44) Da nur die Finanzunternehmen, die für die Zwecke der erweiterten Tests der digitalen Resilienz bestimmt wurden, zu bedrohungsorientierten Penetrationstests verpflichtet werden sollten, sollten die Verwaltungsverfahren und finanziellen Kosten, die mit der Durchführung dieser Tests verbunden sind, von einem kleinen Prozentsatz der Finanzunternehmen getragen werden.

(45) Um die vollständige Abstimmung und allgemeine Kohärenz zwischen den Geschäftsstrategien der Finanzunternehmen einerseits und der Durchführung des IKT-Risikomanagements andererseits zu gewährleisten, sollten die Leitungsorgane der Finanzunternehmen verpflichtet sein, beim Management und bei der Anpassung des IKT-Risikomanagementrahmens und der Gesamtstrategie für die digitale operationale Resilienz eine zentrale und aktive Rolle zu bewahren. Der von den Leitungsorganen heranzuziehende Ansatz sollte sich nicht nur auf die Mittel zur Gewährleistung der Resilienz der IKT-Systeme konzentrieren, sondern auch Menschen und Prozesse durch eine Reihe von Leit- und Richtlinien einbeziehen, die auf jeder Unternehmensebene und bei allen Mitarbeitern ein starkes Bewusstsein für Cyberrisiken und die Verpflichtung zur Einhaltung einer strengen Cyberhygiene auf allen Ebenen hervorrufen. Die letztliche Verantwortung des Leitungsorgans für das Management des IKT-Risikos eines Finanzunternehmens sollte in einem übergeordneten Prinzip dieses umfassenden Ansatzes bestehen, das sich weiter im kontinuierlichen Engagement des Leitungsorgans bei der Kontrolle der Überwachung des IKT-Risikomanagements niederschlägt.

(46) Darüber hinaus geht der Grundsatz der uneingeschränkten und letztlichen Verantwortung des Leitungsorgans für das Management der IKT-Risiken des Finanzunternehmens mit der Notwendigkeit einher, einen bestimmten Umfang von IKT-Investitionen und ein Gesamtbudget sicherzustellen, die das Finanzunternehmen in die Lage versetzen, ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(47) Aufbauend auf einschlägigen internationalen, nationalen und branchenspezifischen bewährten Verfahren, Leitlinien, Empfehlungen und Konzepten für das Management von Cyberrisiken werden mit dieser Verordnung eine Reihe von Prinzipien gefördert, die die allgemeine Struktur des IKT-Risikomanagements erleichtern. Solange die wichtigsten von Finanzunternehmen eingerichteten Kapazitäten die verschiedenen in dieser Verordnung vorgesehenen Aufgaben im IKT-Risikomanagement (Ermittlung, Schutz und Prävention, Erkennung, Reaktion und Wiederherstellung, Lernen sowie Weiterentwicklung und Kommunikation) angehen, sollte es den Finanzunternehmen folglich freistehen, IKT-Risikomanagementmodelle zu verwenden, die anders gegliedert oder kategorisiert sind.

(48) Um mit einer sich rasch ändernden Bedrohungslage Schritt zu halten, sollten Finanzunternehmen auf dem neuesten Stand befindliche IKT-Systeme unterhalten, die zuverlässig sind und nicht nur die Verarbeitung der für die Erbringung ihrer Dienste erforderlichen Daten, sondern auch ausreichende technologische Resilienz gewährleisten können, damit Finanzunternehmen in angemessener Weise auf zusätzliche Verarbeitungserfordernisse aufgrund angespannter Marktbedingungen oder anderer ungünstiger Umstände reagieren können.

(49) Effiziente Pläne zur Fortführung der Geschäftstätigkeit und für die Wiederherstellung sind erforderlich, damit Finanzunternehmen IKT-bezogenen Vorfällen, insbesondere Cyberangriffen, prompt und zügig entgegenwirken können, indem Schäden begrenzt werden und die Wiederaufnahme von Tätigkeiten und Maßnahmen für die Wiederherstellung im Einklang mit ihren Richtlinien für Datensicherung Vorrang erhalten. Eine solche Wiederaufnahme sollte jedoch die Integrität und Sicherheit der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten in keiner Weise gefährden.

(50) Mit dieser Verordnung wird Finanzunternehmen zwar ermöglicht, ihre Vorgaben für die Wiederherstellungszeit (recovery time objective) und die Wiederherstellungspunkte (recovery point objective) flexibel und daher so festzulegen, dass Art und Kritikalität der jeweiligen Funktion sowie etwaige spezifische geschäftliche Erfordernisse in vollem Umfang berücksichtigt werden, allerdings sollte bei der Festlegung dieser Vorgaben auch die Durchführung einer Bewertung der potenziellen Gesamtauswirkungen auf die Markteffizienz vorgeschrieben sein.

(51) Die Urheber von Cyberangriffen neigen dazu, finanzielle Gewinne direkt an der Quelle zu erzielen, sodass Finanzunternehmen weitreichenden Folgen ausgesetzt sind. Um zu verhindern, dass IKT-Systeme ihre Integrität einbüßen oder nicht verfügbar werden, und somit zu vermeiden, dass vertrauliche Daten eingesehen oder physische IKT-Infrastrukturen beschädigt werden, sollte die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen erheblich verbessert und gestrafft werden. Die Meldung IKT-bezogener Vorfälle sollte für alle Finanzunternehmen harmonisiert werden, indem sie verpflichtet werden, ihren jeweils zuständigen Behörden direkt Bericht zu erstatten. Unterliegt ein Finanzunternehmen der Aufsicht von mehr als einer zuständigen nationalen Behörde, so sollten die Mitgliedstaaten eine einzige zuständige Behörde als Adressat einer solchen Meldung benennen. Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 des Rates ([19]) als bedeutend eingestuft werden, sollten die Meldungen den zuständigen nationalen Behörden übermitteln, die sie anschließend an die Europäische Zentralbank (EZB) weiterleiten sollten.

(52) Die direkte Meldung sollte Finanzaufsichtsbehörden den direkten Zugang zu Informationen über schwerwiegende IKT-bezogene Vorfälle ermöglichen. Finanzaufsichtsbehörden sollten Einzelheiten über schwerwiegende IKT-bezogene Vorfälle wiederum an Nicht-Finanzbehörden (z. B gemäß der Richtlinie (EU) 2022/2555 benannte zuständige Behörden und zentrale Anlaufstellen, nationale Datenschutzbehörden und Strafverfolgungsbehörden bei schwerwiegenden IKT-bezogenen Vorfällen strafrechtlicher Art) weiterleiten, um diese Behörden für diese Vorfälle zu sensibilisieren und bei CSIRT gegebenenfalls die unverzügliche Unterstützung von Finanzunternehmen zu erleichtern. Darüber hinaus sollten die Mitgliedstaaten festlegen können, dass Finanzunternehmen selbst derartige Informationen an Behörden außerhalb des Finanzdienstleistungsbereichs weitergeben sollten. Diese Informationsflüsse sollten es Finanzunternehmen ermöglichen, rasch von allen einschlägigen technischen Informationen, der Beratung über Abhilfemaßnahmen und den anschließenden Folgemaßnahmen dieser Behörden zu profitieren. Die Informationen über schwerwiegende IKT-bezogene Vorfälle sollten wechselseitig gelenkt werden: Die Finanzaufsichtsbehörden sollten dem Finanzunternehmen alle erforderlichen Rückmeldungen oder Orientierungshilfen geben, während die ESA anonymisierte Daten über Cyberbedrohungen und Schwachstellen im Zusammenhang mit einem Vorfall austauschen sollten, um eine umfassende kollektive Verteidigung zu unterstützen.

(53) Zwar sollten alle Finanzunternehmen verpflichtet sein, Sicherheitsvorfälle zu melden, es ist jedoch davon auszugehen, dass diese Verpflichtung sie nicht alle in gleicher Weise betrifft. Die einschlägigen Wesentlichkeitsschwellen sowie die Fristen für die Meldung sollten im Rahmen delegierter Rechtsakte auf der Grundlage der von den ESA zu entwickelnden technischen Regulierungsstandards gebührend angepasst werden, um nur schwerwiegende IKT-bezogene Vorfälle abzudecken. Darüber hinaus sollten die Besonderheiten von Finanzunternehmen bei der Festlegung der Fristen für die Meldepflichten berücksichtigt werden.

(54) Diese Verordnung sollte Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute verpflichten, alle zuvor gemäß der Richtlinie (EU) 2015/2366 gemeldeten zahlungsbezogenen Betriebs- oder Sicherheitsvorfälle zu melden, unabhängig von der Art des IKT-Vorfalls.

([19]) Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (ABl. L 287 vom 29.10.2013, S. 63).

(55) Die ESA sollten beauftragt werden, die Durchführbarkeit und die Bedingungen für eine mögliche Zentralisierung von Meldungen über IKT-bezogene Vorfälle auf Unionsebene zu bewerten. Eine solche Zentralisierung könnte in einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle bestehen, die die entsprechenden Meldungen entweder direkt entgegennimmt und die zuständigen nationalen Behörden automatisch benachrichtigt oder lediglich die von den zuständigen nationalen Behörden übermittelten einschlägigen Meldungen zentralisiert und somit eine Koordinierungsfunktion wahrnimmt. Die ESA sollten beauftragt werden, in Absprache mit der EZB und der ENISA einen gemeinsamen Bericht über die Machbarkeit der Einrichtung einer einheitlichen EU-Plattform auszuarbeiten.

(56) Um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen und im Einklang sowohl mit den einschlägigen internationalen Standards (z. B. die „G7 Fundamental Elements for Threat-Led Penetration Testing“ (Grundzüge bedrohungsorientierter Penetrationstests der G7-Staaten)) als auch den in der Union angewandten Rahmen (z. B. TIBER-EU), sollten Finanzunternehmen ihre IKT-Systeme und ihre Mitarbeiter mit IKT-bezogenen Verantwortungen regelmäßig auf die Effizienz ihrer Fähigkeiten für Prävention, Erkennung, Reaktion und Wiederherstellung hin testen, um potenzielle IKT-Schwachstellen aufzudecken und zu beseitigen. Um den Unterschieden Rechnung zu tragen, die zwischen und in den verschiedenen Finanzteilsektoren bei der Abwehrbereitschaft von Finanzunternehmen im Bereich der Cybersicherheit bestehen, sollten die Tests eine breite Palette von Instrumenten und Maßnahmen umfassen, die von der Bewertung grundlegender Anforderungen (z. B. Bewertungen und Überprüfungen der Schwachstellen, Analysen von Open-Source-Software, Bewertungen der Netzwerksicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen, soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests oder End-to-End-Tests) bis hin zu erweiterten Tests anhand von TLPT reichen. Diese erweiterten Tests sollten nur für Finanzunternehmen vorgeschrieben werden, die aus IKT-Perspektive ausgereift genug sind, um sie angemessen durchführen zu können. Folglich sollten die in dieser Verordnung vorgeschriebene Tests der digitalen operationalen Resilienz für die Finanzunternehmen, die die Kriterien dieser Verordnung erfüllen (zum Beispiel große systemrelevante Kreditinstitute mit ausgereifter IKT, Börsen, Zentralverwahrer und zentrale Gegenparteien), ausgedehnter sein als für andere Finanzunternehmen. Gleichzeitig sollten die Tests der digitalen operationalen Resilienz anhand von TLPT für Finanzunternehmen, die in zentralen Finanzdienstleistungsteilsektoren tätig sind und eine systemrelevante Rolle spielen (zum Beispiel Zahlungen, Banken sowie Clearing und Abrechnung), mehr Relevanz und für andere Teilsektoren (zum Beispiel Vermögensverwalter, Ratingagenturen usw.) weniger Relevanz besitzen.

(57) Grenzübergreifend tätige Finanzunternehmen, die die Niederlassungs- oder Dienstleistungsfreiheit in der Union ausüben, sollten in ihrem Herkunftsmitgliedstaat eine einheitliche Reihe von Anforderungen für erweiterte Tests (z. B. TLPT) erfüllen, die sich auf die IKT-Infrastrukturen in allen Rechtsordnungen erstrecken sollten, in denen die grenzüberschreitende Finanzgruppe innerhalb der Union tätig ist, sodass diesen grenzüberschreitend tätigen Finanzgruppen nur in einer Rechtsordnung entsprechende IKT-bezogene Testkosten entstehen.

(58) Um das Fachwissen zu nutzen, das bestimmte zuständige Behörden bereits erworben haben, insbesondere im Zusammenhang mit der Umsetzung von TIBER-EU, sollte es den Mitgliedstaaten durch diese Verordnung ermöglicht werden, auf nationaler Ebene eine einzige staatliche Behörde zu benennen, die im Finanzsektor für alle TLPT-bezogenen Fragen zuständig ist, oder — falls keine solche Behörde benannt wurde — die entsprechenden zuständigen Behörden zu benennen, die die Wahrnehmung von TLPT-bezogenen Aufgaben einer anderen zuständigen nationalen Finanzbehörde übertragen.

(59) Da Finanzunternehmen nach dieser Verordnung nicht verpflichtet sind, mit einem einzigen bedrohungsorientierten Penetrationstest alle kritischen oder wichtigen Funktionen abzudecken, sollte es den Finanzunternehmen freistehen, jeweils festzulegen, welche und wie viele kritische oder wichtige Funktionen im Rahmen dieser Tests geprüft werden sollten.

(60) Gebündelte Tests im Sinne dieser Verordnung — bei denen verschiedene Finanzunternehmen an einem TLPT teilnehmen und ein IKT-Drittdienstleister zu diesem Zweck direkt vertragliche Vereinbarungen mit einem externen Tester eingehen kann — sollten nur dann zulässig sein, wenn gerechtfertigt von nachteiligen Auswirkungen auf die Qualität oder Sicherheit derjenigen Dienstleistungen ausgegangen werden kann, die der IKT-Drittdienstleister für Kunden erbringt, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, oder auf die Vertraulichkeit von mit diesen Dienstleistungen in Verbindung stehenden Daten. Gebündelte Tests sollten auch Schutzvorkehrungen unterliegen (Leitung durch ein benanntes Finanzunternehmen, Abgleich der Anzahl der teilnehmenden Finanzunternehmen), damit ein strenges Testverfahren für diejenigen beteiligten Finanzunternehmen gewährleistet ist, die den Zielen des TLPT gemäß dieser Verordnung gerecht werden.

(61) Um die auf Unternehmensebene verfügbaren internen Ressourcen zu nutzen, sollte der Einsatz interner Tester zur Durchführung von TLPT gemäß dieser Verordnung gestattet sein, sofern eine aufsichtliche Genehmigung vorliegt, keine Interessenkonflikte bestehen und ein regelmäßiger Wechsel (jeweils nach drei Tests) im Einsatz von internen und externen Testern stattfindet, wobei es sich zudem bei dem Anbieter der Bedrohungsanalyse im Rahmen der TLPT stets um ein Unternehmen außerhalb des betreffenden Finanzunternehmens handeln muss. Die Durchführung von TLPT sollten weiterhin uneingeschränkt in der Verantwortung der Finanzunternehmen liegen. Die von den Behörden ausgestellten Bescheinigungen sollten ausschließlich dem Zweck der gegenseitigen Anerkennung dienen und sollten weder Folgemaßnahmen ausschließen, die erforderlich sind, um IKT-Risiken, denen das Finanzunternehmen ausgesetzt ist, anzugehen, noch sollten sie als aufsichtliche Billigung der IKT-Risikomanagement- und -minderungsfähigkeiten eines Finanzunternehmens betrachtet werden.

(62) Um eine solide Überwachung des IKT-Drittparteienrisikos im Finanzsektor zu gewährleisten, sind eine Reihe grundsatzbasierter Regeln festzulegen, um Finanzunternehmen bei der Überwachung der Risiken anzuleiten, die im Zusammenhang mit an IKT-Drittdienstleister ausgelagerten Funktionen — insbesondere mit IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen — sowie ganz allgemein im Zusammenhang mit jeglichen Abhängigkeiten von IKT-Drittdienstleistern entstehen.

(63) Um der Komplexität der verschiedenen IKT-Risikoquellen und dabei zugleich der Vielzahl und Vielfalt der Anbieter technologischer Lösungen, die eine reibungslose Erbringung von Finanzdienstleistungen ermöglichen, gerecht zu werden, sollte diese Verordnung für ein breites Spektrum von IKT-Drittdienstleistern gelten, darunter Anbieter von Cloud-Computing-Diensten, Software, Datenanalysediensten und Anbieter von Rechenzentrumsdienstleistungen. Da Finanzunternehmen alle Arten von Risiken — auch im Zusammenhang mit innerhalb einer Finanzgruppe beschafften IKT-Dienstleistungen — wirksam und kohärent ermitteln und managen sollten, sollte zudem klar herausgestellt werden, dass Unternehmen, die Teil einer Finanzgruppe sind und IKT-Dienstleistungen vorwiegend für ihr Mutterunternehmen oder für Tochterunternehmen oder Zweigniederlassungen ihres Mutterunternehmens erbringen, sowie Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen erbringen, ebenfalls als IKT-Drittdienstleister im Sinne dieser Verordnung gelten sollten. Angesichts der zunehmenden Abhängigkeit des sich entwickelnden Marktes für Zahlungsdienste von komplexen technischen Lösungen sowie angesichts neu entstehender Arten von Zahlungsdiensten und zahlungsbezogenen Lösungen sollten diejenigen Teilnehmer des Ökosystems für Zahlungsdienste, die Zahlungsabwicklungstätigkeiten durchführen oder Zahlungsinfrastrukturen betreiben, ebenfalls als IKT-Drittdienstleister im Sinne dieser Verordnung gelten, mit Ausnahme von Zentralbanken, die Zahlungs- oder Wertpapierliefer- und -abrechnungssysteme betreiben, und von staatlichen Behörden, die IKT-bezogene Dienste im Zusammenhang mit Funktionen des Staates bereitstellen.

(64) Ein Finanzunternehmen sollte jederzeit die volle Verantwortung für die Einhaltung seiner Verpflichtungen aus dieser Verordnung tragen. Die Finanzunternehmen sollten bei der Überwachung der Risiken, die auf Ebene der IKT-Drittdienstleister entstehen, einen verhältnismäßigen Ansatz verfolgen, indem Art, Umfang, Komplexität und Bedeutung ihrer IKT-bezogener Abhängigkeiten und die Kritikalität oder Bedeutung der Dienste, Prozesse oder Funktionen, die den vertraglichen Vereinbarungen unterliegen, letztlich je nach Sachlage anhand einer sorgfältigen Bewertung jeglicher potenzieller Auswirkungen auf die Kontinuität und Qualität von Finanzdienstleistungen auf Einzel- und Gruppenebene gebührend berücksichtigt werden.

(65) Die Durchführung einer solchen Überwachung sollte nach einem strategischen Ansatz für das IKT-Drittparteienrisiko erfolgen, der durch die Annahme einer eigenen Strategie für das von IKT-Drittdienstleistern ausgehende Risiko durch das Leitungsorgan des Finanzunternehmens formalisiert wird, und zwar auf der Grundlage einer kontinuierlichen Überprüfung aller Abhängigkeiten von IKT-Drittdienstleistern. Um die Aufsichtsbehörden für Abhängigkeiten von IKT-Drittdienstleistern zu sensibilisieren und die Arbeiten im Zusammenhang mit dem durch diese Verordnung geschaffenen Überwachungsrahmen weiter zu unterstützen, sollten sämtliche Finanzunternehmen verpflichtet werden, ein Informationsregister mit allen vertraglichen Vereinbarungen betreffend die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden, zu führen. Die Finanzaufsichtsbehörden sollten in der Lage sein, das vollständige Register oder bestimmte Abschnitte des Registers anzufordern und somit wesentliche Informationen zu erhalten, die ein umfassenderes Verständnis der IKT-bezogenen Abhängigkeiten von Finanzunternehmen ermöglichen.

(66) Dem förmlichen Abschluss vertraglicher Vereinbarungen sollte eine gründliche Analyse vor Vertragsabschluss zugrunde liegen und diesem vorausgehen, insbesondere indem der Fokus auf Aspekte wie die Kritikalität oder Bedeutung der durch den geplanten IKT-Vertrag unterstützten Dienste, die erforderlichen aufsichtlichen Genehmigungen oder sonstigen Bedingungen, das damit verbundene mögliche Konzentrationsrisiko sowie die Anwendung der Sorgfaltspflicht bei der Auswahl und Bewertung von IKT-Drittdienstleistern gelegt wird, und indem potenzielle Interessenkonflikte bewertet werden. Betreffen vertragliche Vereinbarungen kritische oder wichtige Funktionen, so sollten Finanzunternehmen darauf achten, dass IKT-Drittdienstleister die aktuellsten und höchsten Standards für die Informationssicherheit anwenden. Die Kündigung vertraglicher Vereinbarungen könnte zumindest

durch eine Reihe von Umständen ausgelöst werden, die Unzulänglichkeiten auf Ebene des IKT-Drittdienstleister erkennen lassen, insbesondere erhebliche Verstöße gegen Rechtsvorschriften oder Vertragsbestimmungen, Umstände, die auf eine potenzielle Änderung der Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen hindeuten, Hinweise auf Schwachstellen beim allgemeinen IKT-Risikomanagement des IKT-Drittdienstleisters oder Umstände, die darauf hinweisen, dass die jeweils zuständige Behörde nicht zu einer wirksamen Beaufsichtigung des Finanzunternehmens in der Lage sind.

(67) Um die systemischen Auswirkungen des Konzentrationsrisikos von IKT-Drittdienstleistern zu anzugehen, wird mit dieser Verordnung eine ausgewogene Lösung angestrebt, indem bei solchen Konzentrationsrisiken ein flexibler und schrittweiser Ansatz verfolgt wird, da jegliche vorgeschriebene starre Obergrenzen oder strenge Beschränkungen die Geschäftstätigkeit behindern und die Vertragsfreiheit beeinträchtigen können. Finanzunternehmen sollten ihre geplanten vertraglichen Vereinbarungen gründlich prüfen, um die Wahrscheinlichkeit des Auftretens eines solchen Risikos zu ermitteln, unter anderem durch fundierte Analysen von Unterauftragsvereinbarungen, insbesondere wenn diese mit IKT-Drittdienstleistern geschlossen werden, die in einem Drittland niedergelassen sind. Um ein ausgewogenes Verhältnis zwischen dem Sachzwang, zum einen die Vertragsfreiheit zu wahren und zum anderen die Finanzstabilität zu gewährleisten, wird es zum gegenwärtigen Zeitpunkt nicht als zweckmäßig erachtet, strenge Obergrenzen und Beschränkungen für die Exposition gegenüber IKT-Drittdienstleistern festzulegen. Was kritische IKT-Drittdienstleister anbelangt, so sollte eine nach dieser Verordnung ernannte federführende Überwachungsbehörde bei der Wahrnehmung ihrer Aufsichtsaufgaben im Kontext des Überwachungsrahmens besonders darauf achten, das Ausmaß der Interdependenzen voll zu erfassen, spezifische Fälle zu ermitteln, in deren Rahmen eine hohe Konzentration kritischer IKT-Drittdienstleister in der Union die Stabilität und Integrität des Finanzsystems der Union belasten dürfte, sowie einen Dialog mit kritischen IKT-Drittdienstleistern zu führen, bei denen dieses spezifische Risiko ermittelt wird.

(68) Um die Fähigkeit eines IKT-Drittdienstleisters, sichere Dienstleistungen für ein Finanzunternehmen ohne nachteilige Auswirkungen auf dessen digitale operationale Resilienz zu erbringen, regelmäßig zu bewerten und zu überwachen, sollten einige wesentliche Vertragsbestandteile mit IKT-Drittdienstleistern harmonisiert werden. Diese Harmonisierung sollte Mindestbereiche abdecken, die — unter dem Gesichtspunkt, dass ein Finanzunternehmen seine digitale Resilienz sicherstellen muss, da es in hohem Maße von der Stabilität, der Funktionalität, der Verfügbarkeit und der Sicherheit der beanspruchten IKT-Dienstleistungen abhängig ist — für eine umfassende Überwachung der von einem IKT-Drittdienstleister möglicherweise ausgehenden Risiken durch das Finanzunternehmen von entscheidender Bedeutung sind.

(69) Bei der Neuaushandlung vertraglicher Vereinbarungen zwecks Angleichung an die Anforderungen dieser Verordnung sollten Finanzunternehmen und IKT-Drittdienstleister sicherstellen, dass die in dieser Verordnung vorgesehenen wesentlichen Vertragsbestimmungen berücksichtigt werden.

(70) Die Begriffsbestimmung der „kritischen oder wichtigen Funktion“ im Sinne dieser Verordnung schließt auch die Begriffsbestimmung der „kritischen Funktionen“ im Sinne von Artikel 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates ([20]) ein. Dementsprechend sind die gemäß der Richtlinie 2014/59/EU als kritisch eingestuften Funktionen in der Begriffsbestimmung der kritischen Funktionen im Sinne dieser Verordnung ebenfalls erfasst.

(71) Ungeachtet der Kritikalität oder Bedeutung der von dem IKT-Drittdienstleister unterstützten Funktion sollte in den vertraglichen Vereinbarungen insbesondere eine Spezifikation der vollständigen Beschreibungen von Funktionen und Dienstleistungen sowie von Orten, an denen solche Funktionen bereitgestellt werden und Daten verarbeitet werden sollen, vorgesehen sein; ferner sollten Beschreibungen der Dienstleistungsgüte enthalten sein. Andere wesentliche Elemente um einem Finanzunternehmen die Überwachung des IKT-Drittparteienrisikos zu ermöglichen, sind die Folgenden: vertragliche Bestimmungen dazu, wie Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit und Schutz personenbezogener Daten durch den IKT-Drittdienstleister gewährleistet werden; Bestimmungen über die einschlägigen Garantien für den Zugang zu sowie die Wiederherstellung und Rückgabe von Daten im Falle einer Insolvenz, Abwicklung oder Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters; Bestimmungen, die den IKT-Drittdienstleister dazu verpflichten, im Falle von IKT-Vorfällen im Zusammenhang mit den erbrachten Dienstleistungen ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu

([20]) Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der Richtlinie 82/891/EWG des Rates, der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (ABl. L 173 vom 12.6.2014, S. 190).

leisten; Bestimmungen über die Verpflichtung des IKT-Drittdienstleisters, uneingeschränkt mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, sowie Bestimmungen über Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und Abwicklungsbehörden.

(72) In Ergänzung zu derartigen vertraglichen Bestimmungen sowie um sicherzustellen, dass Finanzunternehmen die volle Kontrolle über alle von Dritten ausgehenden Entwicklungen behalten, die ihre IKT-Sicherheit beeinträchtigen könnten, sollten die Verträge über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zudem Folgendes vorschreiben: die Spezifikation der vollständigen Beschreibung der Dienstleistungsgüte einschließlich präziser quantitativer und qualitativer Leistungsziele, damit unverzüglich angemessene Korrekturmaßnahmen ergriffen werden können, wenn die vereinbarte Dienstleistungsgüte nicht erreicht werden; die einschlägigen Kündigungsfristen und Meldepflichten des IKT-Drittdienstleisters im Falle von Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters auswirken könnten, die entsprechenden IKT-Dienstleistungen wirksam zur Verfügung stellen; die Anforderung an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu erproben und über Maßnahmen, Instrumente und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die eine sichere Erbringung von Dienstleistungen ermöglichen, sowie sich an dem TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken.

(73) Verträge über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sollten zudem Bestimmungen enthalten, die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten sowie das Recht auf Anfertigung von Kopien regeln, die als wesentliche Instrumente für die laufende Überwachung der Leistung des IKT-Drittdienstleisters durch die Finanzunternehmen dienen, gepaart mit der uneingeschränkten Zusammenarbeit des Drittdienstleisters während der Inspektionen. In gleicher Weise sollte die für das Finanzunternehmen zuständige Behörde auf der Grundlage von Mitteilungen über das Recht verfügen, den IKT-Drittdienstleister vorbehaltlich des Schutzes vertraulicher Informationen zu inspizieren und zu prüfen.

(74) Diese vertraglichen Vereinbarungen sollten ferner spezielle Ausstiegsstrategien vorsehen, die insbesondere verbindliche Übergangszeiträume ermöglichen, in denen die IKT-Drittdienstleister weiterhin die einschlägigen Dienste bereitstellen sollten, um das Risiko von Störungen auf Ebene des Finanzunternehmens zu verringern oder es Letzterem zu ermöglichen, effektiv zu anderen IKT-Drittdienstleistern zu wechseln oder alternativ zu internen Lösungen zu wechseln, die der Komplexität der bereitgestellten IKT-Dienstleistungen entsprechen. Darüber hinaus sollten Finanzunternehmen, die in den Geltungsbereich der Richtlinie 2014/59/EU fallen, sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen solide und im Falle der Abwicklung dieser Finanzunternehmen uneingeschränkt durchsetzbar sind. Daher sollten diese Finanzunternehmen im Einklang mit den Erwartungen der Abwicklungsbehörden sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen abwicklungssicher sind. Solange diese Finanzunternehmen ihren Zahlungsverpflichtungen weiterhin nachkommen, sollten sie neben anderen Anforderungen sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen Klauseln darüber enthalten, dass sie nicht aufgrund einer Umstrukturierung oder Abwicklung gekündigt, ausgesetzt oder geändert werden können.

(75) Darüber hinaus kann die freiwillige Verwendung von Standardvertragsklauseln, die von staatlichen Behörden oder von Organen der Union entwickelt wurden, insbesondere die Verwendung von der Kommission für Cloud-Computing Dienste entwickelten Vertragsklauseln den Finanzunternehmen und IKT-Drittdienstleistern eine zusätzliche Rückversicherung bieten, indem sie die Rechtssicherheit in Bezug auf die Nutzung von Cloud-Computing-Diensten im Finanzsektor in voller Übereinstimmung mit den Anforderungen und Erwartungen des Finanzdienstleistungsrechts der Union erhöht. Die Erarbeitung von Standardvertragsklauseln baut auf Maßnahmen auf, die bereits im FinTech-Aktionsplan von 2018 vorgesehen waren, in dem die Absicht der Kommission angekündigt wurde, die Entwicklung von Standardvertragsklauseln für die Auslagerung von Cloud-Computing-Dienstleistungen durch Finanzunternehmen zu fördern und zu erleichtern, wobei auf den sektorübergreifenden Anstrengungen der Cloud-Interessenträger aufgebaut wird, die die Kommission unter Beteiligung des Finanzsektors unterstützt hat.

(76) Um die Konvergenz und Effizienz von Aufsichtskonzepten in Bezug auf das IKT-Drittparteienrisiko im Finanzsektor zu fördern und um die digitale operationale Resilienz von Finanzunternehmen zu stärken, die bei den IKT-Dienstleistungen, die die Erbringung von Finanzdienstleistungen unterstützen, auf kritische IKT-Drittdienstleister angewiesen sind, und damit zugleich dazu beizutragen, die Stabilität des Finanzsystems der Union und die Integrität des Binnenmarkts für Finanzdienstleistungen zu bewahren, sollten kritische IKT-Drittdienstleister einem Überwachungsrahmen der Union unterliegen. Auch wenn die Einrichtung des Überwachungsrahmens aufgrund des Mehrwerts von Maßnahmen auf Unionsebene und der inhärenten Rolle und der Besonderheiten der Nutzung von

IKT-Dienstleistungen bei der Erbringung von Finanzdienstleistungen gerechtfertigt ist, sollte zugleich daran erinnert werden, dass diese Lösung nur im Kontext dieser Verordnung, die speziell der digitalen operationalen Resilienz im Finanzsektor vorbehalten ist, angemessen erscheint. Ein solcher Überwachungsrahmen sollte hingegen nicht als ein neues Modell für die Beaufsichtigung auf Ebene der Union in den Bereichen Finanzdienstleistungen und -tätigkeiten betrachtet werden.

(77) Der Überwachungsrahmen sollte nur für kritische IKT-Drittdienstleister gelten. Daher sollte es einen Einstufungsmechanismus geben, um dem Ausmaß und der Art der Abhängigkeit des Finanzsektors von solchen IKT-Drittdienstleistern Rechnung zu tragen. Dieser Mechanismus sollte eine Reihe quantitativer und qualitativer Kriterien umfassen, mit denen die Kritikalitätsparameter als Grundlage für die Einbeziehung in den Überwachungsrahmen festgelegt würden. Um eine akkurate Bewertung zu gewährleisten, sollten diese Kriterien unabhängig von der Unternehmensstruktur des IKT-Drittdienstleisters im Falle eines IKT-Drittdienstleisters, der Teil einer größeren Gruppe ist, die gesamte Gruppenstruktur des IKT-Drittdienstleisters berücksichtigen. Einerseits sollten kritische IKT-Drittdienstleister, die aufgrund der Anwendung der oben genannten Kriterien nicht automatisch eingestuft werden, die Möglichkeit haben, sich auf freiwilliger Basis für den Überwachungsrahmen zu entscheiden, andererseits sollten IKT-Drittdienstleister, die bereits Überwachungsmechanismen unterliegen, die die Erfüllung der in Artikel 127 Absatz 2 AEUV genannten Aufgaben des Europäischen Systems der Zentralbanken unterstützen, ausgenommen werden.

(78) Ebenso sollten Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen bereitstellen, zugleich aber der von dieser Verordnung erfassten Kategorie von IKT-Drittdienstleistern angehören, ebenfalls von dem Überwachungsrahmen ausgenommen werden, da sie bereits den Aufsichtsmechanismen unterliegen, die durch das einschlägige Finanzdienstleistungsrecht der Union geschaffen wurden. Wenn zweckmäßig sollten die zuständigen Behörden im Rahmen ihrer Aufsichtstätigkeiten das IKT-Risiko berücksichtigen, das von den IKT-Dienstleistungen bereitstellenden Finanzunternehmen für andere Finanzunternehmen ausgeht. In gleicher Weise sollte aufgrund der auf Gruppenebene bestehenden Risikoüberwachungsmechanismen dieselbe Ausnahme für diejenigen IKT-Drittdienstleister vorgesehen werden, die Dienstleistungen vorwiegend für die ihrer eigenen Gruppe angehörenden Unternehmen erbringen. IKT-Drittdienstleister, die lediglich in einem Mitgliedstaat IKT-Dienstleistungen für Finanzunternehmen bereitstellen, die nur in diesem Mitgliedstaat tätig sind, sollten aufgrund ihrer begrenzten Tätigkeiten und der fehlenden grenzüberschreitenden Auswirkungen ebenfalls von dem Einstufungsmechanismus ausgenommen werden.

(79) Der digitale Wandel im Bereich der Finanzdienstleistungen hat zu einem noch nie da gewesenen Maß an Nutzung und Abhängigkeit von IKT-Dienstleistungen geführt. Da es unvorstellbar geworden ist, Finanzdienstleistungen ohne die Nutzung von Cloud-Computing-Diensten, Softwarelösungen und datenbezogenen Dienstleistungen zu erbringen, ist das Finanzökosystem der Union zwangsläufig immer abhängiger von bestimmten IKT-Dienstleistungen geworden, die von IKT-Dienstleistern bereitgestellt werden. Einige dieser Dienstleister sind Innovatoren bei der Entwicklung und Anwendung IKT-gestützter Technologien und spielen daher eine wichtige Rolle bei der Erbringung von Finanzdienstleistungen oder sind nunmehr fester Bestandteil der Wertschöpfungskette für Finanzdienstleistungen geworden. Somit sind sie für die Stabilität und Integrität des Finanzsystems der Union inzwischen von entscheidender Bedeutung. Diese breite Abhängigkeit von Dienstleistungen, die von kritischen IKT-Drittdienstleistern erbracht werden, in Verbindung mit der Interdependenz der Informationssysteme verschiedener Marktteilnehmer schafft ein unmittelbares und potenziell schwerwiegendes Risiko für das Finanzdienstleistungssystem der Union und für die Kontinuität bei der Erbringung von Finanzdienstleistungen, falls kritische IKT-Drittdienstleister von Betriebsstörungen oder schwerwiegenden Cybervorfällen betroffen sein sollten. Cybervorfälle haben die Besonderheit, dass sie sich im gesamten Finanzsystem potenzieren und erheblich schneller verbreiten können als andere Arten von Risiken, die im Finanzsektor überwacht werden, und sich über Branchen und geografische Grenzen hinweg ausbreiten können. Sie haben das Potenzial, sich zu einer Systemkrise auszuweiten, bei der das Vertrauen in das Finanzsystem aufgrund der Unterbrechung von Funktionen zur Stützung der Realwirtschaft oder aufgrund erheblicher finanzieller Verluste auf ein Niveau sinkt, dem das Finanzsystem nicht standhalten kann oder das gezielte Maßnahmen zur Abfederung schwerer Schocks erfordert. Um zu verhindern, dass diese Szenarien eintreten und dabei die Stabilität und Integrität des Finanzsystems der Union gefährden, ist es von entscheidender Bedeutung, die Aufsichtspraktiken hinsichtlich des IKT-Drittparteienrisikos im Finanzsektor einander anzunähern, insbesondere durch neue Vorschriften, die die Überwachung kritischer IKT-Drittdienstleister in der Union ermöglichen.